Nullification Interpolating Optical Interface for Secure Communications

22 June 2025
Simon Edwards
Research Acceleration Initiative

Introduction

As collimated infrared beams are likely to be utilized on an increasing scale in secure communications, a new paradigm in the prevention of signals intercept is likely to emerge. In addition to previously proposed methods, a novel concept called *nullification interpolation* may be used to allow for data transmitted optically through the air to be made more secure than possible with established methods. This publication also provides yet another solution to the Alice and Bob Paradox in addition to that provided in 19 June 2024.

Abstract

Whereas one branch of optics research seeks to overcome the scattering effects of atmosphere in order to extend the range of a communications protocol (e.g. helical beam transmission,) nullification interpolation seeks to exploit the natural scattering effects of atmosphere in order to prevent the useful intercept of signals and to enable two communicating parties to discover a shared key without the need to communicate the key directly.

In nullification interpolation, data would be encoded in extremely short periods of EM silence purposefully applied to whole waveforms too brief in duration to be discerned without specialized equipment. These brief pauses would, after traveling through a modest quantity of atmosphere, seem to disappear after blending together with neighboring EM. However, adding these periods of EM silence to a signal would leave an enduring and decipherable impression upon the EM even after the periods of absolute silence, taking the form of regions of reduced signal amplitude somewhat longer in duration than the pre-programmed silence. The breadth of this period of reduced amplitude could be expected to increase with proportion to the distance over which the EM travels and its relative magnitude could be expected to decrease.

What makes this approach different from the simple modulation of the amplitude of a signal is that it can be used to cause dynamical patterns of relatively reduced amplitude to emerge at different ranges from the transmitter so that only the recipient receives signal with the intended characteristics. As atmospheric conditions are dynamic, a pulse of light of an established value of frequency and amplitude can be used to take a series of static snapshots of atmospheric conditions vis a vis scattering effects of the light by atmosphere. An adversary eavesdropping at a point halfway between the transmitter and receiver would, in such a scheme, have incomplete information concerning the total optical distortion of the cross-section of atmosphere between the transmitter and receiver and would have insufficient information to decode the data. The system would turn the atmosphere, itself, into an overlapping cypher (layered upon established cyphers) designed to prevent and adversary from making sense of the data. The control signals are

sent both from the data recipient to the sender (the distortion effects are the same regardless of direction) and vice versa and this information is used to enable both the sender to know how to encode the data and to inform the recipient of how to decode it, with the necessary calculations being made with sufficient rapidity to ensure that the state of the atmosphere does not change substantially prior to transmission. This protocol would be analog and, therefore, somewhat fault tolerant, but no so fault tolerant so as to compromise its security.

Conclusion

This approach exploits a basic concept used in atmospheric noise-based random number generation, sc. the measurement of a data point which never repeats and which is different depending upon from whence it is measured. Whereas an atmospheric RNG works by algorithmically mixing signal from four or more antennae in confidential locations, this method allows for the scattering effects of atmosphere to be assessed wholistically between two specific points at one specific time and for these unique and non-repeating characteristics to be used as both its own cypher and as a means of determining how long of a nullification interpolation is required for coherent signal to reach the intended destination so that the minimal possible length of nullification may be used in order to reduce, insofar as is possible, the profile of the encoded data (the information security concept of always using the minimal needed signal strength.) This has as its benefit of conferring the ability to hide the existence of a transmission and to strongly encrypt the transmission, securing the data even if its existence were somehow discovered. Furthermore, as the atmospheric condition-based cypher would be constantly variable, a physical mechanism could prevent any key data from being permanently stored as this process could be carried out within its own closed loop, preventing the theft of the key. Both sender and recipient would make simultaneous observation of the atmosphere (with the aid of itinerant pulses coming from the other) and would independently evaluate the atmospheric conditions without having to communicate their findings with the other. Without the need to communicate the key as such, both parties would have key knowledge, thereby overcoming the Alice and Bob Paradox in addition to ensuring that a random and non-repeating key is utilzied.